



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,965	04/17/2001	Alfred C. She	012.P53011	8500
43831	7590	03/16/2007	EXAMINER	
BERKELEY LAW & TECHNOLOGY GROUP, LLP			TRUONG, THANHNGA B	
1700 NW 167TH PLACE			ART UNIT	PAPER NUMBER
SUITE 240			2135	
BEAVERTON, OR 97006				
			MAIL DATE	DELIVERY MODE
			03/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

**Advisory Action
Before the Filing of an Appeal Brief**

Application No.

09/836,965

Applicant(s)

SHE ET AL.

Examiner

Thanhnga B. Truong

Art Unit

2135

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 29 January 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) The period for reply expires _____ months from the mailing date of the final rejection.

b) The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
 (a) They raise new issues that would require further consideration and/or search (see NOTE below);
 (b) They raise the issue of new matter (see NOTE below);
 (c) They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
 (d) They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).

4. The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. Applicant's reply has overcome the following rejection(s): _____.

6. Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. For purposes of appeal, the proposed amendment(s): a) will not be entered, or b) will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: _____.

Claim(s) objected to: _____.

Claim(s) rejected: _____.

Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.

12. Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____

13. Other: _____.

Thanhnga B. Truong

T. B. Truong
AU 2135

Continuation of 11. does NOT place the application in condition for allowance because:

Applicant argues that:

The combination of Wright, Nakamura, and Coppersmith fail to teach, show, or suggest all the elements of claim 1, concerning incremental deciphering. Incremental deciphering refers to an operation and/or process used in block encryption/decryption as opposed to stream encryption/decryption. It is to be understood that incremental deciphering is the deciphering operation that takes place in a particular round of deciphering. The deciphering is incremental because a round key can only partially decipher the ciphered text block. Application of a multiplicity of round keys, each in its own particular round of deciphering, to the same text block in its successively partially deciphered state can ultimately produce the completely deciphered text block.

Examiner disagrees with the applicant and still maintains that:

Wright teaches a first cipher stream generated from a private key negotiated as a result of a public key exchange is partitioned to form a sequence of secondary keys. The secondary keys are then indexed. In one instance, each plaintext data packet is encrypted with a second cipher streams generated from a different one of the secondary keys. In another instance, a second cipher stream generated from a single secondary key is used to encrypt a plurality of plaintext data packets. A new second cipher stream generated from another one of the secondary keys is then used for encryption following each instance of the loss of a ciphertext data packet. The index is communicated with the ciphertext to identify which secondary key is to be used in generating the second cipher stream needed for decryption. With knowledge of the secondary key to be used, re-synchronization (along with new private key negotiation) at each instance of a ciphertext data packet loss is obviated (see abstract).

Although Wright's Figure 8 describes more details in incrementing with each encryption or decryption process (column 8, lines 48-67 through column 9, lines 1-21), Wright is silent on the capability of how many rounds of cipher processing have been performed. On the other hand, Coppersmith teaches a method and apparatus for advanced byte-oriented symmetric key block cipher with variable length key and block (emphasis added). Furthermore, referring to Figure 3, the first Step 100 is to initialize the iteration counter, "r", to keep track of how many rounds of cipher processing have been performed. At Step 110, a comparison is made between the iteration counter and the number of rounds of processing required. While the iteration counter is less than the number of rounds, the processing will continue on to Step 120. However, if the two values compared are equal, then encryption of the block has completed. It will be understood that the encryption process for each block of data forming the input file is identical, and that the process of Figure 3 is used on each successive block until all blocks of the input file have been encrypted (emphasis added) (column 7, lines 48-59 of Coppersmith). In addition, Coppersmith further teaches, a commonly used cipher is known as the Data Encryption Algorithm ("DEA"). This algorithm was developed by scientists of the International Business Machines Corporation ("IBM"), and formed the basis of a United States federal standard known as the Data Encryption Standard ("DES"), which was adopted in 1977. DES has been in use since that time. A variant of the DES algorithm, known as "Triple DES", was developed to increase the strength of the result over that available with DES. Triple DES uses three rounds of ciphering, with different keys for each of the rounds (emphasis added). After twenty years, many believe that a new stronger, more flexible algorithm is needed. One way to make a cipher stronger is to increase the number of rounds (emphasis added) of ciphering performed: with each successive transformation, the resulting encryption becomes more difficult to break (column 2, lines 20-34 of Coppersmith). Furthermore, another object of the present invention is to provide a solution that allows precomputing the sub-keys to be used for each round of ciphering (emphasis added), in order to minimize the time required for encrypting or decrypting an individual file or message. Still another object of the present invention is to provide a technique whereby the cipher used for encryption and decryption is block-oriented, uses a symmetric key, and uses different sub-keys during each round of ciphering. A further object of the present invention is to provide a technique whereby the cipher uses a variable number of rounds (emphasis added) of processing during encryption and decryption, a variable length block of data as the unit to be encrypted and decrypted, and a variable length key. Allowing these factors to vary will provide the user with choices that will not only affect execution time and strength of security for any given use of the cipher, but will also allow variation between subsequent uses of the cipher, further increasing the difficulty of breaking encrypted data from a given source (column 3, lines 50-67 through column 4, line 1 of Coppersmith). Thus, the combination of teaching between Wright, Nakamura, and Coppersmith teaches the claim subject matter.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of teaching between Wright, Nakamura, Coppersmith, and Adler is sufficient.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., Incremental deciphering refers to an operation and/or process used in block encryption/decryption; and the deciphering is incremental because a round key can only partially decipher the ciphered text block) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Thus, Wright, Nakamura, Coppersmith, and Adler do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Allowable Subject Matter:

Claims 4-9, 13-19, 24-30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.